IV Quantum Computing and Quantum Algorithms

1. The circuit model

a) Classical computation

Use of classical computers (abstractly):

Solve problems $\equiv$ compute functions

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m$$

$$\underline{x} = (x_1, \dots, x_n) \longmapsto f(x_1, \dots, x_n)$$

The function f depends on the problem we want to solve, $\underline{x}$ encodes the instance of the problem.

E.g.: Problem = multiplication : $(a, b) \longmapsto a \cdot b$

$$\underline{x} = (\underline{x}^1, \underline{x}^2) \longmapsto f(\underline{x}) = \underline{x}^1 \cdot \underline{x}^2$$

encoded in binary

Problem = Factorization:

$\underline{x}$: integer; $f(\underline{x})$: list of prime factors (suitably encoded)

More precisely:

Each problem is encoded by a family of functions $f \equiv f^{(n)} : \{0,1\}^n \to \{0,1\}^m$, with $m = \text{poly}(n)$, $n \in \mathbb{N}$ – one for each input size.

i.e.: m grows at most polynomially with n (technically, $\exists \alpha > 0$ s.th. $\frac{m}{n^\alpha} \to 0$).

(Technical point: It must be possible to "construct the functions $f^{(n)}$ systematically and efficiently", see later!)

Which ingredients do we need to compute a general function f?

(i) $f : \{0,1\}^n \longrightarrow \{0,1\}^m$

$$f(\underline{x}) = (f_1(\underline{x}), f_2(\underline{x}), \dots, f_m(\underline{x}))$$

where $f_k(\underline{x}) : \{0,1\}^n \longrightarrow \{0,1\}$

$\Rightarrow$ can restrict analysis to Boolean functions

$$f : \{0,1\}^n \longrightarrow \{0,1\}.$$

(ii) Define $L = \{\underline{y} \mid f(\underline{y}) = 1\} = \{\underline{y}^1, \underline{y}^2, \dots, \underline{y}^\ell\}$.

Define $\underline{\delta}_{\underline{y}}(\underline{x}) = \begin{cases} 0 \,; & \underline{x} \neq \underline{y} \\ 1 \,; & \underline{x} = \underline{y} \end{cases}$ ← bitwise equality!

Then, $f(\underline{x}) = \underline{\delta}_{\underline{y}^1}(\underline{x}) \vee \underline{\delta}_{\underline{y}^2}(\underline{x}) \vee \dots \vee \underline{\delta}_{\underline{y}^\ell}(\underline{x})$

"$\vee$": logical "<u>or</u>":

(0 ≡ "false",
1 ≡ "true")

$0 \vee 0 = 0$
$0 \vee 1 = 1$
$1 \vee 0 = 1$
$1 \vee 1 = 1$

"$\vee$" is <u>associative</u>:

$$a \vee b \vee c := (a \vee b) \vee c = a \vee (b \vee c)$$

and <u>commutative</u>: $a \vee b = b \vee a$.

(iii) Define bitwise δ:

$$\delta_y(x) = \begin{cases} 0 : & y \neq x \\ 1 : & y = x \end{cases}$$

Then,

$$\delta_{\underline{y}}(\underline{x}) = \delta_{y_1}(x_1) \wedge \delta_{y_2}(x_2) \wedge \ldots \wedge \delta_{y_n}(x_n)$$

"$\wedge$": logical "and":

($0 \equiv$ "false",
$1 \equiv$ "true")

$0 \wedge 0 = 0$
$0 \wedge 1 = 0$
$1 \wedge 0 = 0$
$1 \wedge 1 = 1$

"$\wedge$" is associative & commutative;

"$\wedge$" & "$\vee$" are distributive:

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c).$$

(In essence, same rules as $\wedge \rightarrow \cdot$, $\vee \rightarrow +$)

(iv)

$$\delta_y(x) = \begin{cases} x & \text{if } y = 1 \\ \neg x & \text{if } y = 0 \end{cases}$$

Logical "not": $\neg 0 = 1$

$\neg 1 = 0$

Combine (i) – (iv):

Any $f(\underline{x})$ can be constructed from 4 ingredients:

"and", "or", "not" gates,

plus a "copy" gate $x \mapsto (x, x)$.

This is called a universal gate set.

(Note: In fact, already either $\neg(x \wedge y)$ "nand", or $\neg(x \vee y)$ "nor" are universal, together with "copy".)

This gives rise to the

Circuit model of computation:

The functions $f \equiv f^{(i)}$ which we can compute are constructed by concatenating gates from a simple universal gate set (e.g. and/or/not/copy) sequentially in time (i.e., there are no loops allowed). This gives rise to a circuit for $f^{(n)}$.

The difficulty ("computational hardness") of a problem in the circuit model is measured by the number $K(n)$ of elementary gates needed to compute $f^{(n)}$ ($\hat{=}$ # of time steps).

We often distinguish two qualitatively different regimes:

$K(n) \sim \mathrm{poly}(n)$: efficiently solvable (class P)
easy problems

$K(n) \gg \mathrm{poly}(n)$ – e.g. $K(n) \sim \exp(n^\alpha)$:

hard problem

(Technical note: We must suppose that the circuits used for $f^{(n)}$ are <u>uniform</u>, i.e. they can be generated efficiently – e.g. by a simple n-independent computer program. More formally, $f^{(n)}$ should be generated by a Turing machine.)

<u>Example:</u>

f = <u>Multiplication</u>:

Efficient:

$$
\begin{array}{r}
\overbrace{10110}^{\ell} \times \overbrace{10011}^{\ell'} \\
\hline
10110 \\
10110 \\
10110 \\
\hline
\underbrace{110100010}_{\ell \times \ell' \text{ additions:}}
\end{array}
\left.\right\} \ell'
$$

$O(\ell\ell') \sim O(n^2)$ gates.

f: <u>Factorization</u>.

E.g.: Sieve of Eratosthenes:

$\{0,1\}^n \rightarrow$ try about $\sqrt{2^n} \sim 2^{n/2}$ cases

$\Longrightarrow$ hard / exp. scaling.

No efficient algorithm known!

Is a typical problem easy or hard?

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

$$\#\text{ of different } f: \quad 2^{\underbrace{(2^n)}_{\#\text{ of inputs}}}$$

$f(\underline{x}) = \begin{cases} 0 \\ 1 \end{cases}$ for each input

But: there are only $c^{\text{poly}(n)}$ circuits of length poly(n)!

# of elem. gates

$\Rightarrow$ As n gets large, most f cannot be computed efficiently (i.e. with poly(n) operations).

Does the computational power depend on the gate set?

NO! By definition, any universal gate set can simulate any other gate set with constant overhead!

<u>Remark</u>: There is a wide range of alternative models of computation, some more and some less realistic:

- CPU
- parallel computers
- "Turing machines" – tape + read/write head
- cellular automata
- ... and lots of exotic models ...

<u>But</u>: All known "reasonable" models of computation can simulate each other with poly(n) overhead

$\Longrightarrow$ same computational power (in the sense above).

<u>Church-Turing-Thesis</u>: All reasonable models of computation have the same computational power.

b) Reversible circuits

For quantum computing – coming soon – we will use the circuit model.

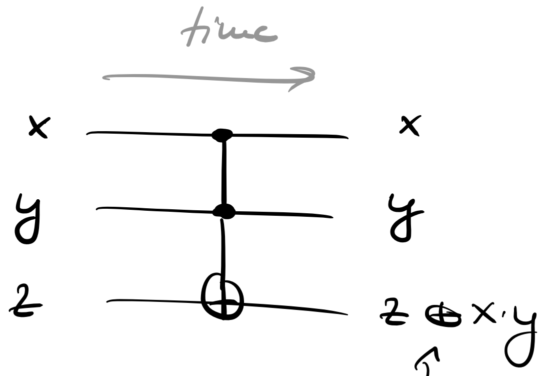
Gates will be replaced by unitaries.

But: Unitaries are reversible, while classical gates (and, or) are irreversible.

Could such a model even do classical computations – i.e., can we find a universal gate set with only reversible gates?

YES! – Classical computation can be made reversible:

Toffoli gate:



"XOR" = addition mod 2:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

also assoc., comm., & distr. w/ $\wedge$. (like "v")

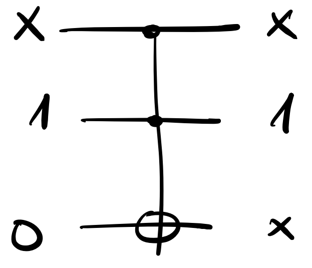
→ Toffoli gate is reversible

(it is its own inverse, since $(z \oplus x\cdot y) \oplus x\cdot y = z$)

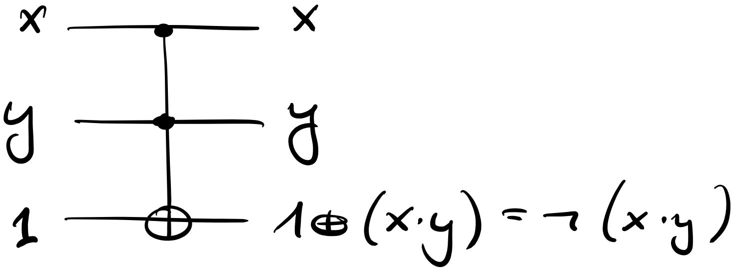
→ Toffoli gate can simulate and/or/not/copy,

by using ancillas in state "0" or "1":

E.g.:



"copy"



"Nand"

⟹ gives reversible universal gate set

(but requires ancillas)

This can be used to compute any $f(\underline{x})$ reversibly,

using ancillas, with essentially the same # of gates:

$$f^R(\underline{x}, y) \longmapsto (\underline{x}, f(\underline{x}) \oplus y)$$

bitwise XOR.

(Idea: Replace any gate by a reversible gate using ancillas. Then XOR the result into the y register. Finally, run the circuit backwards to "uncompute" the ancillas. Ancilla count can be optimized for → cf. Preskill's notes.)

⇒ Everything can be computed reversibly.

But: 3-bit gate is required!

(→ Homework)

c) Quantum Circuits

Most common model for quantum computation:

The circuit model:

- Quantum system consisting of qudits: tensor product structure.
- Universal gate set $S = \{U_1, \dots, U_k\}$ of few-qudit gates (typ. 1- and 2-qudit gates) U_j. (See later for definition of "universal"!)
- Construct circuits by sequentially applying

elements of S to a subset of qubits:

$$|\psi_{out}\rangle = U_T U_{T-1} \cdot \ldots \; U_1 |\psi_{in}\rangle$$

U_j acting on subset of qubits

- Initial state:

$$|\psi_{in}\rangle = |x_1\rangle|x_2\rangle \ldots |x_n\rangle \overbrace{|0\rangle|0\rangle \ldots |0\rangle}^{\ell}$$

$$= |\underline{x}\rangle|\underline{0}\rangle$$

ancillas

encodes instance of problem

– alternatively, we can also have

$$|\psi_{in}\rangle = |\underline{0}\rangle \equiv |0\rangle^{\otimes \ell}$$

and encode the instance in the circuit.

- At the end of the computation, measure the final state $|\psi_{out}\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$

$\longrightarrow$ outcome $|y\rangle$ w/ prob. $p(y) = |\langle y|\psi_{out}\rangle|^2$

Notes: • This is a probabilistic scheme — it outputs y w/ some prob. $p(y)$. In principle, we should compare to class. probabilistic schemes — see later.

• We need not measure all qubits —

not measuring = tracing = measuring and ignoring outcome

◦ POVMs don't help — we can simulate them (→ Naimark). Similarly, CP maps don't help — we can simulate them (Stinespring + trace ancilla).

◦ Measurements at earlier times don't help: Can always postpone them (they commute). If gate at later time would depend on meas. outcome: This dependence can be realized inside the circuit w/ "controlled gates"

(cf. later + homework)

What gate set should we choose?

- There is a <u>continuum</u> of gates — situation much more rich.

- <u>Different notions of universality</u> exist:

  - <u>exact universality</u>: Any n-qubit gate can be realised <u>exactly</u>.

    → Requires a <u>continuous family</u> of universal gates (counting argument!)

  - <u>approximate universality</u>: Any n-qubit gate can be approximated well by gate set

    (Finite gate set sufficient;

    <u>Solovay-Kitaev-Theorem</u>: ε-approximation (in $\|\cdot\|_\infty$-Norm) of 1-qubit gate requires $O(\mathrm{poly}(\log(1/\varepsilon)))$ gates from a suitable finite set.)

- 1- and -2 qubit gates alone are universal! (cf. classical: 3-bit gates needed!!)

- For approximate universality, almost any ~~single~~ two-qubit gate will do!

  w/ prob. 1.

- More univ. sets: later!

d) Universal gate set

Our exact universal gate set:

(i) 1-qubit rotations about X & Z axis:

$$R_x(\phi) = e^{-iX\phi/2} \quad ; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad X^2 = I$$

$$R_z(\phi) = e^{-iZ\phi/2} \quad ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Z^2 = I.$$

For $M^2 = I$: $e^{-iM\phi/2} = \cos\phi/2 \; I - i\sin\phi/2 \; M$

$$\Longrightarrow \quad R_x(\phi) = \begin{pmatrix} \cos\phi/2 & -i\sin\phi/2 \\ -i\sin\phi/2 & \cos\phi/2 \end{pmatrix}$$

$$R_z(\phi) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}$$

can be understood as rotations on Bloch sphere about X/Z axis by angle ϕ (i.e., rotations in $SO(3) \cong SU(2)/\mathbb{Z}_2$).

Together, R_x and R_z generate all rotations in $SO(3)$ (Euler angles!), and thus in $SU(2)$ up to a phase.

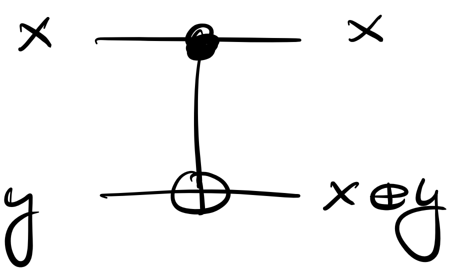
<u>Lemma:</u> For any $U \in SU(2)$,

$$U = e^{i\phi} R_x(\alpha) R_z(\beta) R_x(\gamma) \text{ for some } \phi, \alpha, \beta, \gamma.$$

<u>Proof:</u> <u>Homework.</u>

(ii) <u>one</u> two qubit gate (almost all would do!).

Typically, we use "controlled-NOT" = "CNOT":



$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT flips y iff $x = 1$: <u>classical</u> gate!

Can prove: This gate set can create any n-qubit U exactly (but of course not efficiently – U has $\sim (2^n)^2 = 4^n$ real parameters).

Overview of a number of important gates & identities

(Proof/check: Homework!)

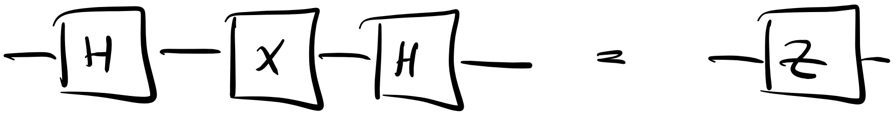
Hadamard gate: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H = H^\dagger ; \quad H^2 = I .$$

$$H R_x(\phi) H = R_z(\phi)$$

$$H R_z(\phi) H = R_x(\phi)$$

Graphical "circuit" notation:

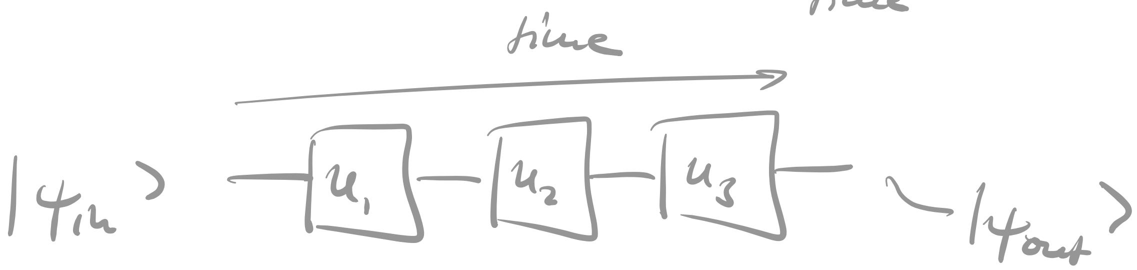


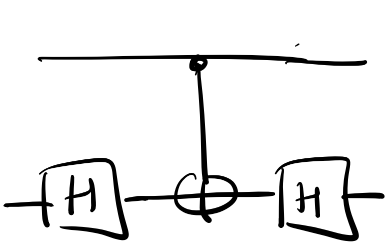
Important:

Matrix notation: time goes right to left

Circuit notation: time goes left to right:

i.e.: $$|\psi_{in}\rangle \longmapsto |\psi_{out}\rangle = \underbrace{U_3 U_2 U_1}_{\xleftarrow{\text{time}}} |\psi_{in}\rangle$$

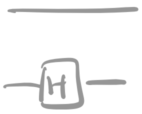




=

$$= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

only applied to 2nd qubit, i.e.:

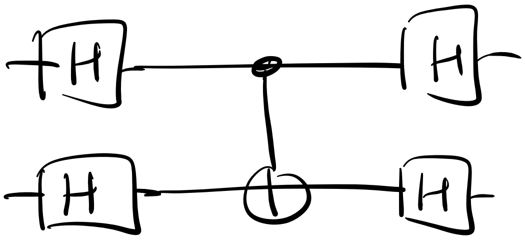


$\equiv I \otimes H.$

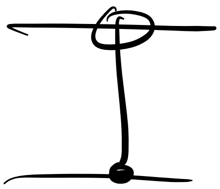
"Controlled-Z"

"Controlled-Phase"

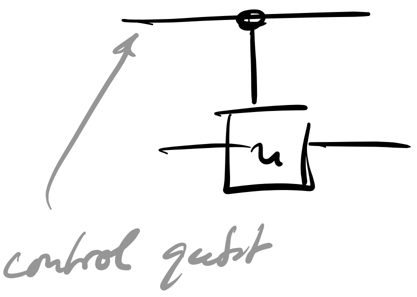
CZ, CPHASE



=



Generally: For a unitary $U \in SU(2)$,

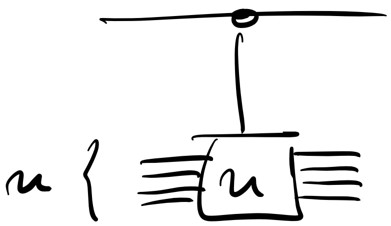


$$= \left(\begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array}\right)$$
$$\underbrace{}_{\text{control } = |0\rangle} \quad \underbrace{}_{\text{control } = |1\rangle}$$

"controlled-U"

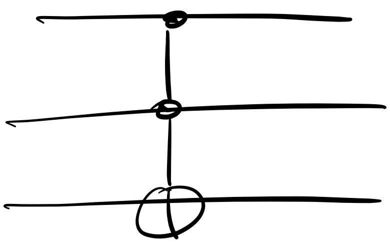
Can be implemented w/ 2 CNOT (→ HW!)

Also for $U \in SU(2^n)$:

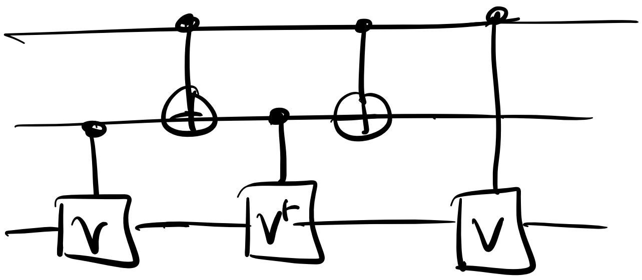


$$= \left(\begin{array}{c|c} I_{2^n} & 0 \\ \hline 0 & U \end{array}\right)$$

Circuit for Toffoli:



$=$

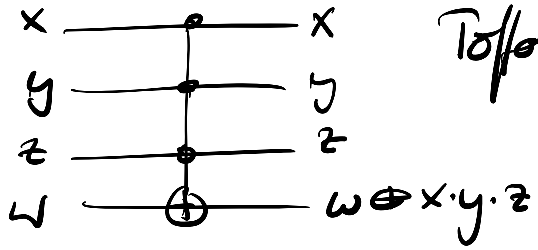


with $V = \frac{1-i}{2}(I + iX)$

U to controlled-U:

Given circuit for U – in particular, a classical reversible circuit – we can also build controlled-U:

Just replace every gate by its controlled-version, in particular Toffoli by



Toffoli w/ 3 controls can be built from normal Toffoli (since class. universal!)

Finally, some <u>further approx. universal gate sets</u>:

- CNOT + 2 random 1-qubit gates
- CNOT + H + $T = R_z(\pi/4)$ ("$\pi/8$ gate")

2. Oracle-based algorithms

a) The Deutsch algorithm

Consider $f: \{0,1\} \longrightarrow \{0,1\}$

Let f be "very hard to compute" – e.g. long circuit

Want to know: Is $f(0) = f(1)$?

(e.g.: will a specific chess move affect result?)

How often do we have to run the circuit for f (= "evaluate f")? — We think of f as a "black box" or "oracle": How many oracle queries are needed?

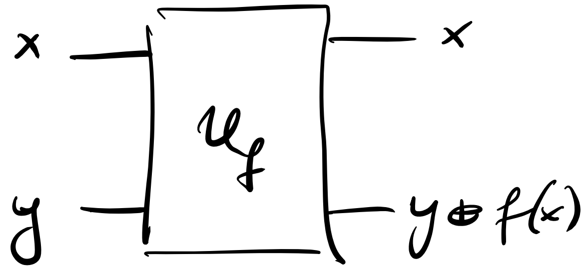
Classically, we clearly need 2 queries:

compute $f(0)$ and $f(1)$.

Can quantum physics help?

Consider reversible implementation of f:

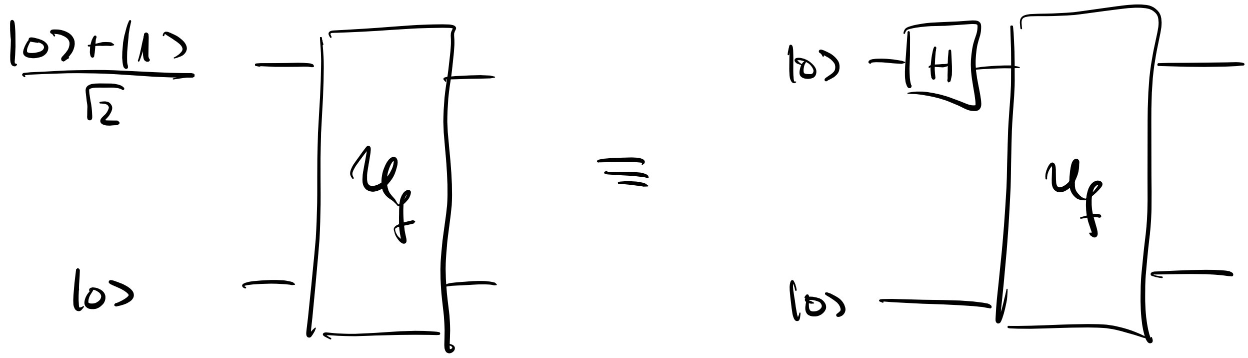
$$f^R: (x,y) \longmapsto (x, y \oplus f(x))$$



$$|x\rangle|y\rangle \longmapsto |x\rangle|y \oplus f(x)\rangle$$

Try to use superpositions as inputs?

First attempt:



$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|0\rangle\right) \xmapsto{\mathcal{U}_f} \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$$

→ Have evaluated f on both outputs!

But how can we extract the relevant information (i.e. do a measurement)?

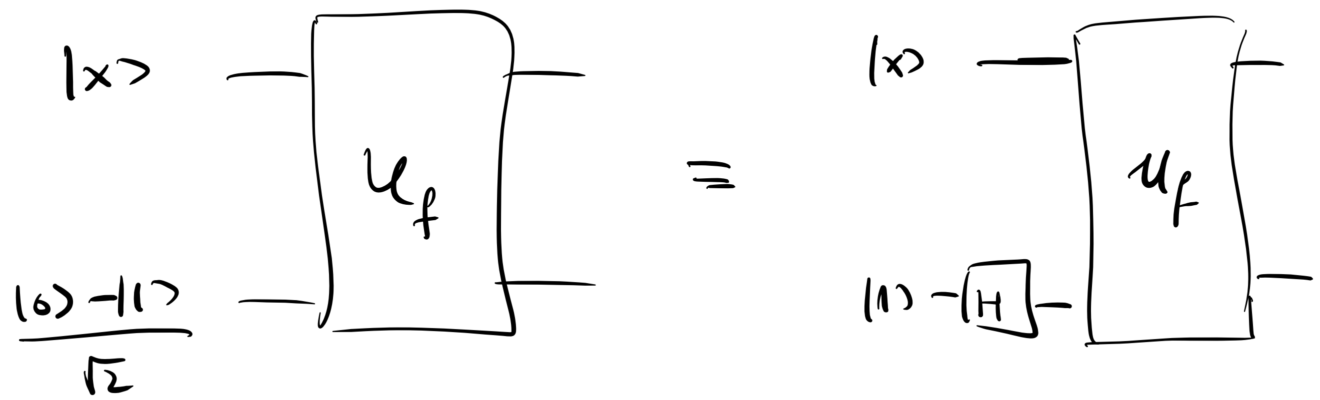
- Meas. in comp. basis: collapse superpos. to one case!
- Generally: $f(0) \neq f(1)$: outputs $\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$,
  $\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$,

$\underline{f(0) = f(1)}$: outputs $|+\rangle|0\rangle$,

$|+\rangle|1\rangle$.

$\Longrightarrow$ not orthogonal, i.e. not (determ.) distinguishable!

<u>Second attempt:</u>



$$|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xmapsto{U_f} |x\rangle\left(\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) =$$

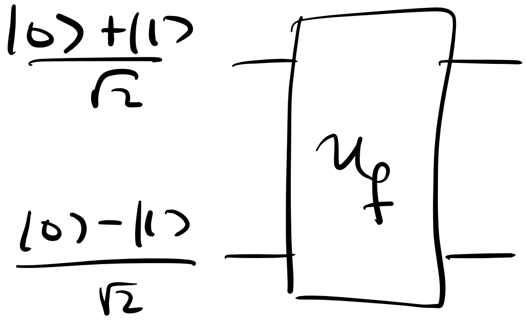
$$= \begin{cases} f(x) = 0 : & |x\rangle \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \\[2ex] f(x) = 1 : & |x\rangle \dfrac{|1\rangle - |0\rangle}{\sqrt{2}} \end{cases}$$

$$= |x\rangle\left[(-1)^{f(x)} \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$= (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Not useful by itself: $f(x)$ only encoded in global phase for each classical input $|x\rangle$.

Combine attempts:



:

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \left(|0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} + |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$= \frac{1}{\sqrt{2}} \left((-1)^{f(0)} |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} + (-1)^{f(1)} |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$= \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Observations:

→ No entanglement created (!)

→ 2nd qubit – the one where U_f outputs the function value – is unchanged (!!)

→ 1st qubit gets a phase $(-1)^{f(x)}$

("phase kick-back technique")

State of 1st qubit:

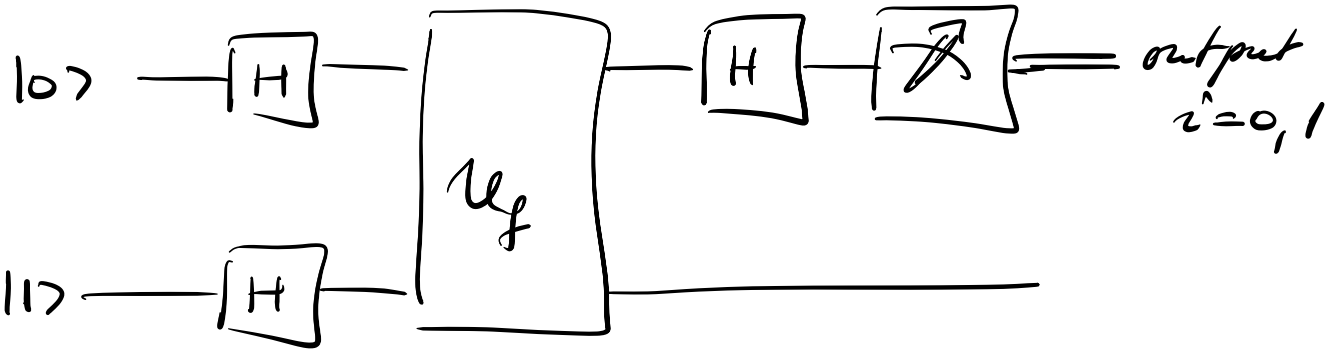
$$f(0) = f(1) \longleftrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$f(0) \neq f(1) \longleftrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

(up to irrelevant global phase)

Orthogonal states! $\Longrightarrow$ measurement of 1st qubit in basis $\{|+\rangle, |-\rangle\}$ (or apply –$\boxed{H}$– & measure in $\{|0\rangle, |1\rangle\}$) allows to decide if $f(0) \overset{?}{=} f(1)$!

Deutsch algorithm:



output $i=0: \Rightarrow f(0) = f(1)$

$i=1: \Rightarrow f(0) \neq f(1)$

One application of U_f has been sufficient!

$\Rightarrow$ Speed-up compared to class. algorithm
(1 vs. 2 oracle queries).

Interesting to note: 2nd qubit never needs to be measured – and it contains no information.

Two main insights:

- Use input $\sum |x\rangle$ to evaluate f on all inputs simultaneously.
- This parallelism alone is not enough – need a smart way to read out the relevant information.

However, a constant speed-up is not that impressive – in particular, it is highly architecture-dependent!

Thus:

b) The Deutsch-Jozsa algorithm

Consider $f: \{0,1\}^n \longrightarrow \{0,1\}$ with promise (i.e., a condition we know is met by f) that

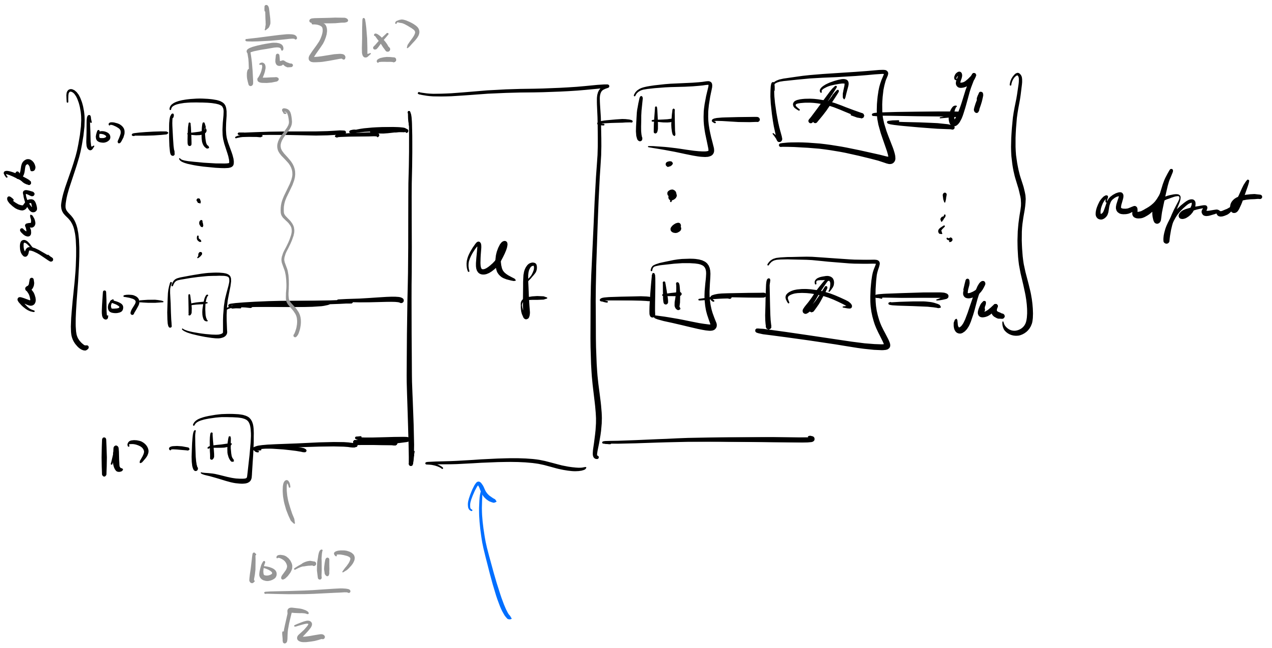
either $f(\underline{x}) = c \quad \forall \underline{x}$ ("f constant")

or $|\{\underline{x} \mid f(\underline{x})=0\}| = |\{\underline{x} \mid f(\underline{x})=1\}|$ ("f balanced")

Want to know: Is f constant or balanced?

How many queries needed?

Use same idea: Input $\sum |x\rangle$ and $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$:



$U_f: |\underline{x}\rangle|y\rangle \longmapsto |\underline{x}\rangle|y \oplus f(x)\rangle$

Before analyzing circuit: What is action of $H^{\otimes n}$?

$$H: \ |x\rangle \longmapsto \frac{1}{\sqrt{2}} \sum_{y=0,1} (-1)^{x \cdot y} |y\rangle$$

$$H^{\otimes n}: \ |x_1, \dots, x_n\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{\underline{y}} (-1)^{x_1 y_1} \cdot \ldots \cdot (-1)^{x_n y_n} |y_1, \dots, y_n\rangle$$

or:

$$|\underline{x}\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum (-1)^{\underline{x} \cdot \underline{y}} |\underline{y}\rangle$$

where $\underline{x} \cdot \underline{y} := x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n$

("scalar product" mod 2).

is NOT a scalar product!

Analysis of circuit:

we omit normalization!

$$|\underline{0}\rangle|1\rangle \xrightarrow{H^{\otimes n} \otimes H} \left(\sum_{\underline{x}} |\underline{x}\rangle\right)\left(|0\rangle - |1\rangle\right)$$

phase kick-back

$$\xrightarrow{U_f} \left(\sum_{\underline{x}} (-1)^{f(\underline{x})} |\underline{x}\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$$\xrightarrow{H^{\otimes n} \otimes I} \left(\sum_{\underline{y}} \underbrace{\sum_{\underline{x}} (-1)^{f(\underline{x}) + \underline{x} \cdot \underline{y}}}_{=: a_{\underline{y}}} |\underline{y}\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$p_{\underline{y}} := |a_{\underline{y}}|^2$ is the probability to measure $\underline{y} = (y_1, \dots, y_n)$.

<u>f constant:</u> $f(\underline{x}) = c$

$$a_{\underline{y}} = (-1)^c \underbrace{\sum_{\underline{x}} (-1)^{\underline{x} \cdot \underline{y}}}_{\propto\, \delta_{\underline{y}, \underline{0}}} = (-1)^c \delta_{\underline{y}, \underline{0}}$$

<u>f balanced:</u>

For $\underline{y} = \underline{0}$: $a_{\underline{0}} = \sum_{\underline{x}} (-1)^{f(\underline{x}) + \underline{x} \cdot \underline{0}}$

$$= \sum_{x} (-1)^{f(\underline{x})} = 0$$

<u>f balanced!</u>

<u>Thus:</u>

Output $\underline{y} = \underline{0}$ $\Longrightarrow$ f constant

Output $\underline{y} \neq \underline{0}$ $\Longrightarrow$ f balanced

$\Longrightarrow$ We can <u>unambiguously</u> <u>distinguish</u> the 2 cases with <u>one query to the oracle for f!</u>

What is the speed-up vs. classical methods?

<u>Quantum:</u> 1 use of f.

<u>Classical:</u> Worst case, we have to determine

$2^{n-1}+1$ values of f to be sure!

$\Rightarrow$ exponential vs. constant!

<u>But:</u> If we are ok to get right answer with very high probability $p = 1 - p_{error}$, then for k queries to f,

$$p_{error} \approx 2 \cdot \underbrace{\left(\frac{1}{2}\right)^k}$$

$\approx$ prob. to get $k\times$ same outcome for balanced f, if $k \ll 2^n$.

<u>i.e.:</u> $k \sim \log(1/p_{error})$.

<u>Randomized classical:</u> Much smaller speed-up vs. randomized classical algorithm (even for exp. small error, $k \sim n$ oracle calls are sufficient.)

c) Simon's algorithm

... will give us a true exponential speedup (also rel. to randomized class. algorithms) in terms of oracle queries!

Oracle: $f : \{0,1\}^n \to \{0,1\}^n$

with promise:

$\exists\, \underline{a} \neq \underline{0}$ s.th. $f(\underline{x}) = f(\underline{y})$ exactly if $\underline{y} = \underline{x} \oplus \underline{a}$.

("hidden periodicity")

Task: Find $\underline{a}$ by querying f.

Classical: Need to query $f(\underline{x}_i)$ until pair $\underline{x}_i, \underline{x}_j$ with $f(\underline{x}_i) = f(\underline{x}_j)$ is found.

Roughly: k queries $x_1, \dots, x_k \to \sim k^2$ pairs,

for each pair: prob $(f(\underline{x}_i) = f(\underline{x}_j)) \approx 2^{-n}$

$\Rightarrow P_{\text{success}} \sim k^2\, 2^{-n}$

$\Rightarrow$ need $k \sim 2^{cn}$ queries!

Quantum algorithm (Simon's algorithm):

i) Start with $\frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |\underline{x}\rangle = H^{\otimes n} |\underline{0}\rangle$

ii) Apply $U_f : |\underline{x}\rangle|y\rangle \longmapsto |\underline{x}\rangle|y \oplus f(\underline{x})\rangle$

$$U_f : \left(\frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |\underline{x}\rangle_A\right)|\underline{0}\rangle_B \longmapsto \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |\underline{x}\rangle_A |f(\underline{x})\rangle_B$$

iii) Measure B. $\Rightarrow$ Collapse onto random $f(\underline{x}_0)$ (and thus random $\underline{x}_0$).

$\Rightarrow$ Register A collapses onto

$$\frac{1}{N} \sum_{\underline{x}: f(\underline{x}) = f(\underline{x}_0)} |x\rangle = \frac{1}{\sqrt{2}}\left(|\underline{x}_0\rangle + |\underline{x}_0 \oplus \underline{a}\rangle\right)$$

— How can we extract a? —

(Meas. in comp. basis $\rightarrow$ collapse on rand. x_0: useless.)

iv) Apply $H^{\otimes n}$ again:

$$\boxed{H^{\otimes n}|\underline{x}\rangle \propto \sum_{y} (-1)^{\underline{x}\cdot y}|y\rangle}$$

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}\left(|\underline{x}_0\rangle \oplus |\underline{x}_0 \oplus a\rangle\right)\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y} \underbrace{\left[(-1)^{\underline{x}_0 \cdot y} + (-1)^{(\underline{x}_0 + \underline{a}) \cdot y} \right]}_{} |y\rangle$$

$\rightarrow \underline{a} \cdot y = 0 \implies \quad = 2 \cdot (-1)^{\underline{x}_0 \cdot y}$

$\underline{a} \cdot y = 1 \implies \quad = 0$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{y : \underline{a} \cdot y = 0} (-1)^{\underline{x}_0 \cdot y} |y\rangle$$

v) Measure in comp. basis:

$\implies$ obtain <u>random y</u> s.th. $\underline{a} \cdot y = 0$.

$(n-1)$ lin. indep. vectors y_i (over $\mathbb{Z}_2$) s.th. $\underline{a} \cdot y_i = 0$ allow to determine $\underline{a}$ (solve lin. eq. – e.g. Gaussian elimination).

Space of lin. dep. vectors of k vectors grows as 2^k

$\implies O(1)$ chance to find randomly a lin. indep. vector

$\implies O(n)$ random y are enough

$\Rightarrow$ $O(n)$ oracle queries are enough (on average)

Classical: 2^{cn} queries
Quantum: $c' \cdot n$ queries

$\Big\}$ exponential speed-up !

(in terms of oracle queries)

Notes:

- We don't have to measure B — we never use the outcome! (But: Derivation easier this way!)
- $H^{\otimes n} \hat{=}$ (discrete) Fourier transform over $\mathbb{Z}_2^{\times n}$

  $\longrightarrow$ period finding via Fourier transform

3. The quantum Fourier transform, period finding, and Shor's factoring algorithm

Can we go beyond Fourier trafo on $\mathbb{Z}_2$ (to $\mathbb{Z}_N$, for $N \sim 2^n$)?

- What is the right transformation?
- Can it be implemented efficiently?
- What is it good for?

Further reading:
A. Ekert and R. Jozsa,
Quantum computation and Shor's factoring algorithm.
Rev. Mod. Phys **68**, 733 (1996)
https:///doi.org/10.1103/RevModPhys.68.733

a) The Quantum Fourier Transform

Discrete Fourier trafo (FT) on $\mathbb{C}^N$:

$$x = (x_0, \dots, x_{N-1}) \in \mathbb{C}^N$$

$$y = (y_0, \dots, y_{N-1}) \in \mathbb{C}^N$$

FT: $\mathcal{F}: x \longmapsto y$ s.th. $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \, jk/N}$

Definition QFT

$$\boxed{|j\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \, jk/N} |k\rangle}$$

Observe:

$$\sum_j x_j |j\rangle \xrightarrow{QFT} \sum_{jk} x_j\, e^{2\pi i jk/N} |k\rangle = \sum y_k |k\rangle$$

i.e.: QFT acts as discrete FT on amplitudes!

Computational cost of classical FT:

- $O(N^2)$ operations.
- $N \sim 2^n \Rightarrow$ exponential in # of bits in N.
- Fast FT (FFT): only $O(N \log N)$,
  but still exponential!
- $O(N)$ is lower bound: minimal time to
  even just output y_k!

Will see: QFT can be implemented on a quantum
state in $O(n^2)$ steps

$\rightarrow$ exponential speedup!

(But only useful if input is give as q. state!)

Step I: Rewrite QFT in binary

- Consider case $N = 2^n$.
- Write j etc. in binary:

$$j = j_1 j_2 j_3 \cdots j_n = j_1 \cdot 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$$

- "Decimal" point notation:

$$0.j_\ell j_{\ell+1} \cdots j_n = \frac{1}{2} j_\ell + \frac{1}{4} j_{\ell+1} + \ldots + \frac{1}{2^{n-\ell+1}} j_n$$

Then:

$$|j\rangle \longmapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n - 1} e^{2\pi i\, j \cdot k/2^n} |k\rangle$$

$= 0.k_1 k_2 \ldots k_n$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right)} |k_1, \ldots, k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \left[\bigotimes_{\ell=1}^{n} \left(e^{2\pi i j\, k_\ell 2^{-\ell}} |k_\ell\rangle \right) \right]$$

$$= \bigotimes_{\ell=1}^{n} \left[\frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} e^{2\pi i j k_\ell 2^{-\ell}} |k_\ell\rangle \right]$$

$$= \bigotimes_{\ell=1}^{n} \frac{1}{\sqrt{2}}\left[|0\rangle + e^{2\pi i j 2^{-\ell}}|1\rangle\right] = \ldots$$

$$\to \quad j \cdot 2^{-\ell} = \underbrace{j_1 j_2 \cdots j_{n-\ell}}_{\text{integer}} \cdot j_{n-\ell+1} \cdots j_n$$

$$e^{2\pi i (j \cdot 2^{-\ell})} = e^{2\pi i \cdot (\text{integer} + 0.j_{n-\ell+1} \cdots j_n)}$$

$$= e^{2\pi i \cdot 0.j_{n-\ell+1} \cdots j_n}$$

$$\ldots = \frac{|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_{n-1} j_n}|1\rangle}{\sqrt{2}} \otimes \ldots$$

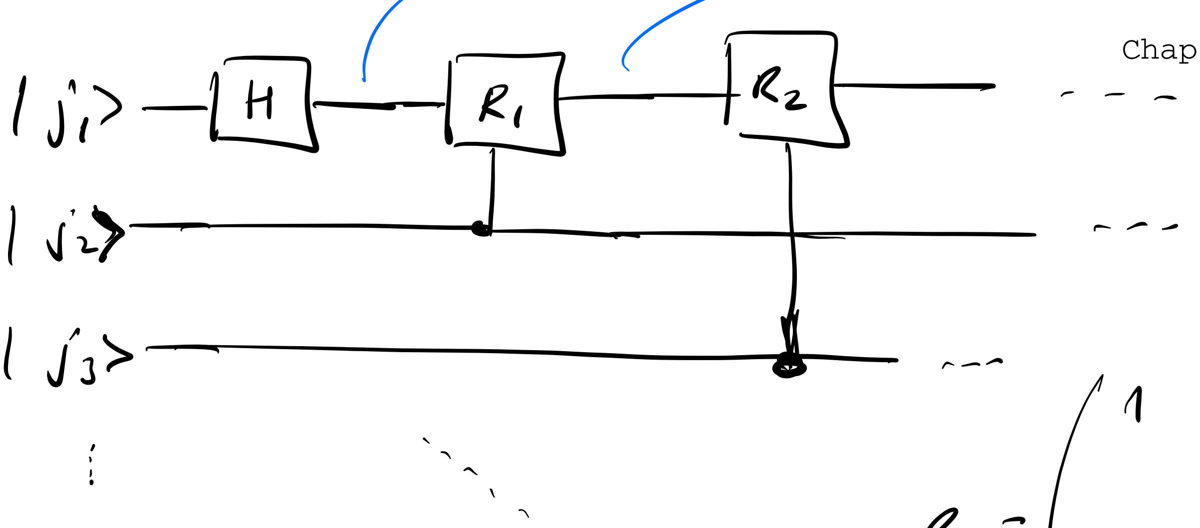
$$\ldots \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}}$$

Step II: Implement this as a circuit.

Consider first only rightmost term:

$$\frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + \overbrace{e^{2\pi i\, j_1/2}}^{(-1)^{j_1}} e^{2\pi i\, j_2/4} \cdot e^{2\pi i\, j_3/8} \cdots |1\rangle}{\sqrt{2}}$$

$$|0\rangle + e^{2\pi i\, j_1/2}|1\rangle \qquad |0\rangle + e^{2\pi i\, j_1/2} e^{2\pi i\, j_2/4}|1\rangle$$



$$R_d = \begin{pmatrix} 1 & \\ & e^{2\pi i \cdot 2^{-(d+1)}} \end{pmatrix}$$

Action of gates:

$$H: |j_1\rangle \longmapsto |0\rangle + e^{2\pi i\, 0.j_1} |1\rangle$$

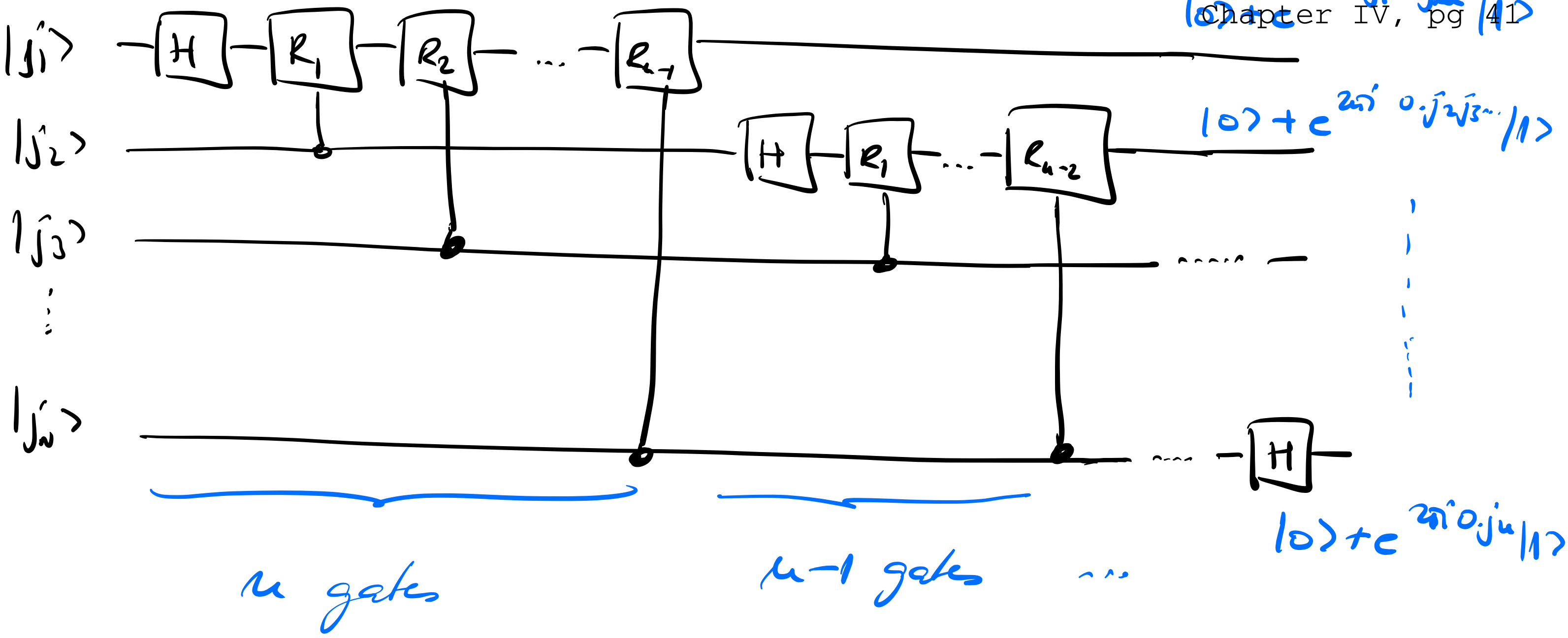
$$C\text{-}R_1: \left(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\right)|j_2\rangle \longmapsto \left(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\right)|j_2\rangle$$

$$C\text{-}R_2: \left(|0\rangle + e^{2\pi i\, 0.j_1 j_2}\right)|j_2\rangle|j_3\rangle \longmapsto \left(|0\rangle + e^{2\pi i\, 0.j_1 j_2 j_3}|1\rangle\right)|j_2\rangle|j_3\rangle$$

$\vdots$ and so on.

$\longrightarrow$ Outputs the n-th qubit of the QFT on 1st qubit.

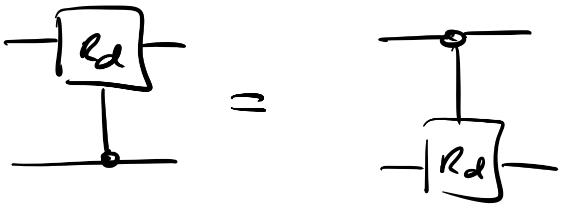
Continue in this vein:



<u>Gate count:</u> $\frac{n(n+1)}{2} = O(n^2)$ gates!

<u>Notes:</u>

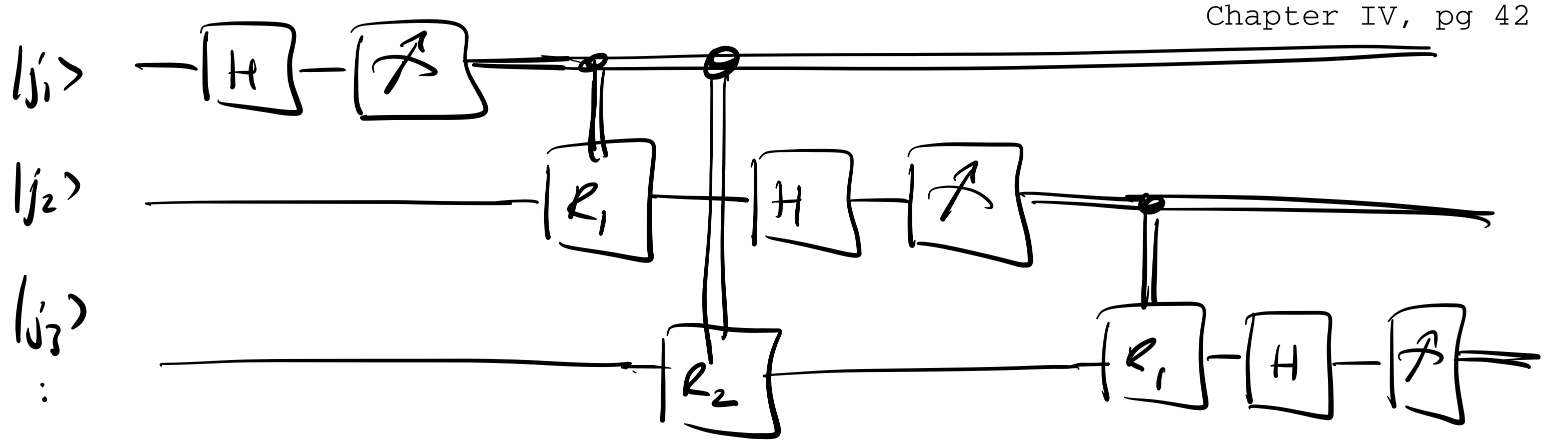
- Output qubits in <u>reverse order</u> (can re-order if needed: $n/2$ swaps).

- 

$\Rightarrow$ can flip C-R_d gates

Then, upper line acts as <u>control</u> in comp. basis.

$\Rightarrow$ If we <u>measure</u> directly after QFT in comp. basis, we can measure <u>before</u> the C-R_d gates & control them classically:



Only one-qubit gates needed (!!)

("Where is the quantum-ness?")

b) Period finding

Application of QFT: Find period of a function?
(cf. Simon's algorithm)

Consider a periodic function $f: \mathbb{N} \to \{0, \dots, M-1\}$, such that $\exists r > 0$ with

$$f(x) = f(x+r), \text{ and } f(x) \neq f(y) \text{ otherwise.}$$

On a computer, we can only compute f on a truncated input,

$$f: \underbrace{\{0, \dots, N-1\}}_{=\{0,1\}^n} \longrightarrow \underbrace{\{0, \dots, M-1\}}_{=\{0,1\}^m}$$

(In particular, the periodicity of f is broken across the boundary, if we think of $f(x+r) \equiv f((x+r) \bmod N)$)

Can we find r better than classically?

(i.e., with much less than $\sim r$ queries to f)

Choose n such that $2^n \gg r$

will make this specific later.
Goal: imperfection at end. negligible.

Implement U_f on quantum computer as before:

$$U_f : |x\rangle_A |y\rangle_B \longmapsto |x\rangle_A |y \oplus f(x)\rangle_B$$

Algorithm:

① Hadamard on A, then U_f:

$$\frac{1}{2^{n/2}} \sum |x\rangle_A |0\rangle_B \xmapsto{U_f} \frac{1}{2^{n/2}} \sum |x\rangle_A |f(x)\rangle_B$$

② Measure B register. For result $|f(x_0)\rangle_B$,

A collapses to

$$\frac{1}{\sqrt{k_0}} \sum_{k=0}^{k_0-1} |x_0 + kr\rangle$$

– here, $0 \le x_0 < r$, and $\frac{2^u}{r} - 1 < k_0 \le \frac{2^u}{r}$.

(3) Apply QFT:

$$\mapsto \frac{1}{2^{u/2}\sqrt{k_0}} \sum_{k=0}^{k_0-1} \sum_{\ell=0}^{2^u-1} e^{2\pi i (x_0 + kr)\ell/2^u} |\ell\rangle_A$$

$$= \sum_{\ell=0}^{2^u-1} \underbrace{e^{2\pi i x_0 \ell/2^u} \underbrace{\sum_{k=0}^{k_0-1} \frac{1}{2^{u/2}\sqrt{k_0}} e^{2\pi i k r \ell/2^u}}_{=: \hat{a}_\ell}}_{=: a_\ell} |\ell\rangle_A$$

(4) Measure in computational basis:

$|\hat{a}_\ell|^2$: probability to obtain outcome ℓ

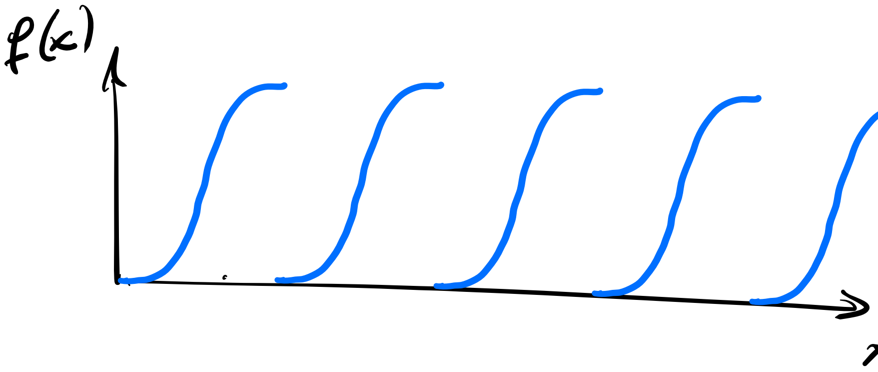
<u>Intuitively:</u> $\hat{a}_\ell \propto \sum_k e^{2\pi i k (r\ell/2^u)}$

peaked around points ℓ where $\frac{r\ell}{2^u}$ is close to an integer!

(→ Will quantify this in a moment!)

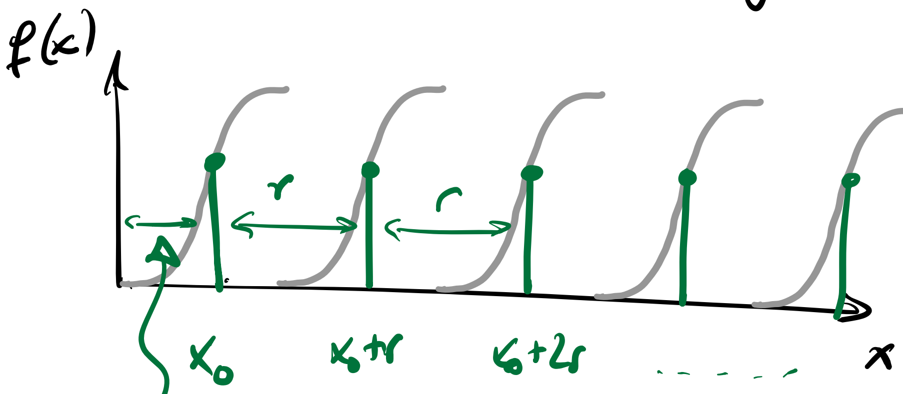
Intuitive picture:

(General features of Fourier transforms — nothing quantum!)



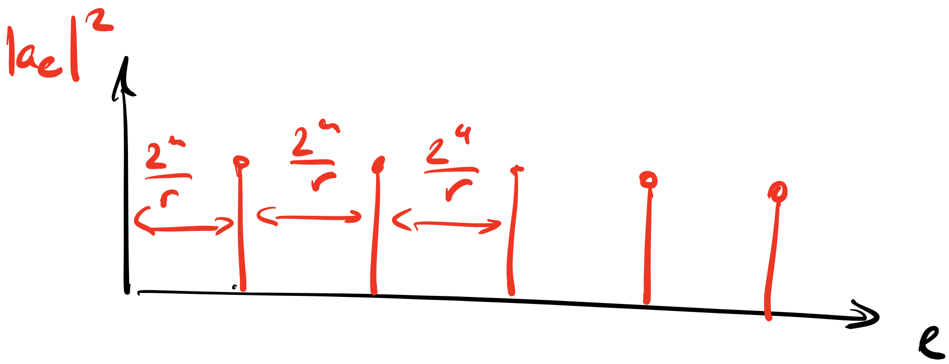
periodic function

after meas. of B $\longrightarrow x_0$



unknown offset x_0 !

Fourier trafo



unknown offset: absorbed in phase of a_ℓ !

$\Rightarrow$ can determine multiple of $\frac{2^n}{r}$ by measuring ℓ (How to get r? Later!)

Detailed analysis of $|a_\ell|^2$:

How much total weight is on all $|a_\ell|^2$ with

$$\ell = \frac{2^n}{r}\cdot s + \delta_s \;;\quad \delta_s \in \left(-\tfrac{1}{2};\tfrac{1}{2}\right];\quad s=0,\dots,r-1$$

(i.e. only those ℓ which are closest to $\frac{2^n}{r}\cdot s$

$\rightarrow$ from those, we can uniquely infer $\frac{2^n}{r}\cdot s$.)

$$\text{Then, } \hat{a}_\ell = \frac{1}{2^{n/2}\sqrt{k_0}} \sum_{k=0}^{k_0-1} e^{2\pi i k \overbrace{\left(s+\frac{r}{2^n}\delta_s\right)}^{\equiv r\ell/2^n}}$$

$$= \frac{1}{2^{n/2}\sqrt{k_0}} \frac{e^{2\pi i \frac{r}{2^n}\delta_s k_0}-1}{e^{2\pi i \frac{r}{2^n}\delta_s}-1}$$

... since $\frac{2^n}{r}-1 < k_0 \leq \frac{2^n}{r}$, and $r \ll 2^n$:

$$\frac{k_0 r}{2^n} = 1-\varepsilon\,,\quad 0\leq \varepsilon < \frac{r}{2^n} \ll 1.$$

$$= \frac{1}{2^{n/2}\sqrt{k_0}} \; \frac{e^{2\pi i \delta_s (1-\varepsilon)} - 1}{e^{2\pi i \frac{r}{2^n}\delta_s} - 1}$$

$$\Rightarrow \quad |a_e|^2 = \frac{1}{2^n k_0}\left(\frac{\overbrace{\sin\left(\pi \delta_s (1-\varepsilon)\right)}^{\sin x \,\geq\, \frac{x}{\pi/2} \text{ on relev. interval}}}{\underbrace{\sin\left(\frac{\pi r}{2^n}\delta_s\right)}_{\sin x \,\leq\, x}} \right)^2$$

$$\geq \frac{1}{2^n k_0} \; \frac{\dfrac{\cancel{\pi^2}\,\cancel{\delta_s^2}\,(1-\varepsilon)^2}{\pi^2/4}}{\dfrac{\cancel{\pi^2}\, r^2}{(2^n)^2}\,\cancel{\delta_s^2}}$$

$$= \frac{4}{\pi^2}\,\frac{1}{r}\;\frac{(1-\varepsilon)^2}{\underbrace{\dfrac{k_0 r}{2^n}}_{\geq 1-\varepsilon}}$$

$$= \frac{4}{\pi^2}\,\frac{1}{r}\,(1-\varepsilon) \approx \frac{4}{\pi^2}\,\frac{1}{r}$$

(can be easily made more quantitative, using $\varepsilon < \frac{r}{2^n}$!)

Since $s = 0, \ldots, r-1$: Total probability that

$\left| \ell - \frac{2^n}{r} s \right| \leq \frac{1}{2}$ for one such s: $p \geq \frac{4}{\pi^2} \approx 0.41$

With sufficiently high probability – we will see that we can <u>check</u> success and thus repeat until we succeed! – we obtain an ℓ s.th. $\ell = \frac{2^n}{r} s + \delta_s$, and thus,

$$\frac{\ell}{2^n} \approx \frac{s}{r},$$

where s is chosen uniformly at random.

If we choose $r \ll 2^n$ suitably, there is only <u>one</u> such ratio $\frac{s}{r}$ with $\left| \ell - \frac{2^n}{r} s \right| \leq 1/2$, and it can be found efficiently. (See further reading.)

Specifically, it suffices to choose $N = 2^n = (2^m)^2 = M^2$, i.e. $n = 2m$, and since $M \geq r$: $2^n \gg 2^{n/2} > r$.

If s and r are co-prime, i.e. $\gcd(r,s)=1$, we can infer r from $\frac{s}{r}$. This happens with probability at least $p(\gcd(s,r)=1) \geq 1/\log r \geq \frac{2}{\log 2} \cdot \frac{1}{n}$.

(at least all primes $2 \leq s < r$ are good, and density of primes goes as $1/\log r$.)

$\Rightarrow$ with $O(n)$ iterations, we find a s coprime with r.

Once we have used this to obtain a guess for r, we can test whether $f(x) = f(x+r)$, and repeat until success!

$\Rightarrow$ Efficient algorithm for period finding.

$\sim O(n)$ applications of f required!

c) Application: Factoring Algorithm

Factoring: Given $N \in \mathbb{N}$ (not prime), find

$f \in \mathbb{N}$, $f \neq 1$, such that $f \mid N$.

"f divides N"

(Note: Primality of N can be checked efficiently.)

This can be solved efficiently if we have an efficient method for period finding!

Sketch of algorithm:

(1) Select a random a, $2 \leq a < N$.

If $\gcd(a,N) > 1 \Rightarrow$ done, $f = \gcd(a,N)$!

eff. computable!

Thus: Assume $\gcd(a,N) = 1$.

(2) Denote by r the smallest $x>0$ such that

$$a^x \bmod N = 1.$$

– that is, the period of

$$f_{N,a}(x) := a^x \bmod N$$

r is called the <u>order of a mod N.</u>

(<u>Note</u>: Some $z>1$ s.th. $a^z \bmod N = 1$ must exist

since

$\exists\, x,y \in \{1,\dots,N\}:\ a^x \equiv a^y \bmod N$ (counting possibilities)

$\Rightarrow a^x(1-a^{y-x}) \equiv 0 \bmod N$

$\Rightarrow N \mid (a^x(1-a^{y-x}))$

$\overset{\gcd(a,N)=1}{\Longrightarrow} N \mid (1-a^{y-x})$

$\Rightarrow a^{y-x} \equiv 1 \bmod N$ ∎)

Recall: "<u>Efficient</u>" means "<u>polynomial in # of digits of N</u>"

Furthermore, $f_{N,a}(x)$ can be <u>computed efficiently</u>:

Using $x = x_{m-1}2^{m-1} + x_{m-2}2^{m-2} + \dots$,

$$a^x \bmod N = \underbrace{\left(a^{(2^{m-1})}\right)}\left.^{x_{m-1}}\right. \cdot \left(a^{(2^{m-2})}\right)^{x_{m-2}} \cdot \ldots \bmod N$$

eff. computable via repeated squaring mod N:

$$a \mapsto a^2 \bmod N \mapsto \underbrace{a^4 \bmod N}_{\equiv (a^2 \bmod N)^2 \bmod N} \mapsto \ldots,$$

by doing "mod N" in each step the numbers don't require an exp. number of digits:

$O(n)$ multiplications of n-digit numbers.

$\Rightarrow$ r can be found efficiently with a quantum computer!

(3) Assume for now r even:

$$a^r \bmod N = 1$$

$$\Leftrightarrow N \mid (a^r - 1),$$

$$\Leftrightarrow N \mid (a^{r/2}+1)(a^{r/2}-1)$$

However, we also know that $N \nmid (a^{r/2} - 1)$,

since otherwise $a^{r/2} \bmod N = 1$ ↯ does not divide

$\Rightarrow$ <u>either</u> $N \mid a^{r/2} + 1$

<u>or</u> N has non-trivial common factors with <u>both</u> $a^{r/2} \pm 1$.

$\Rightarrow 1 \neq f := \gcd(N, a^{r/2}+1) \mid N$

$\Rightarrow$ found a <u>non-trivial factor f of N!</u>

$\Rightarrow$ Algorithm will succeed as long as

(i) r even

(ii) $N \nmid (a^{r/2}+1)$

This can be shown to happen with prob. $\geq 1/2$ for a random choice of a (see further reading) – <u>unless</u> either N is even (can be checked efficiently),

or $N = p^k$, p prime

(can also be checked efficiently by taking roots; there are only $O(\log(N))$ roots which one has to check!)

- and in both cases, this gives a non-trivial factor!

$\Rightarrow$ <u>efficient Quantum Algorithm for Factoring.</u>

<u>"Shor's algorithm"</u>